UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/476,037	12/31/1999	RODNEY A. KORN	042390.P6098	7224

7590 04/14/2004

GREGORY D CALDWELL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN L L P
12400 WILSHIRE BOULEVARD SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
GURSHMAN, GRIGORY	
ART UNIT	**PAPER NUMBER**
2132	8

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/476,037	**Applicant(s)** KORN R.	
	Examiner Grigory Gurshman	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9,13,16,17 and 19-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9,13,16,17 and 19-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 9, 13-17,19-39 refer to new claims and amended claims.

2. Referring to claims 9, 23 and 25, Applicant argues that Atkinson does not teach every element of the claims. Examiner points out that the broad but reasonable interpretation of the claim language is applied. In light of that, examiner points out that Atkinson teaches "signing the control program, comprising the public key" -see Fig.4.

3. With regard to claims 16 and 24, Applicant argues that Atkinson does not teach claim elements. Examiner points out that Atkinson teaches the following:

a) verifying a public key cryptography signature associated with a control program is shown in Fig. 6.

b) computing a hashed value for each executable command in a script;

A cryptographic digest or hash is determined for the code as it is received.

(col 3, line 18-19),

c) decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

d) the digest is compared to the digest included in the publisher signature.

(col 3, line 19-20) c) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script;

the digest is compared to the digest included in the publisher signature.

(col 3, line 19-20)

e) executing the executable commands in the, script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands. A match between the digests confirms the integrity of the code. A dialog is then rendered by the recipient computer indicating who is providing the code and the certification agency that has authenticated the identity of the publisher (col 3, line 20-24). The dialog can be rendered by browser application, for example, and can include user queries as to whether to open or run executable file. (col 8, line 24-26).

Examiner points out that Atkinson does anticipate independent claims 9,16,23,24 and 25.

4. Regarding claim 17, Applicant argues that Ogilvie does not teach or suggest the features missing from Atkinson. Examiner points out that Ogilvie disclosed that the system may encrypt (or reencrypt) the information during an optional encrypting step 312 to secure the sensitive information.

The disclosure conditions, formats, and/or destinations may also be encrypted (col 10, line 57-59). Possible formats include plaintext, digitally signed, encrypted, XML or HTML, and other formats for electronic documents (col 10, line 19-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the script with a symmetric encryption key to secure the sensitive data as taught in Ogilvie.

5. Referring to claim 19 Applicant also argues that McManis does not teach or suggest the features missing from Atkinson. Examiner disagrees and point out that McManis disclosed a single digital signature for each program module, and the associated message digest is computed using a hash function (col 4, line 55-57). The digital signature must match corresponding message digest computed by the verifier in order the verifier to return a verification confirmation message, and then to execute the program procedure calls (col 4, line 66-67, continue to the first line of col 7, abstract). The Procedure A calls Procedure B, then Procedure B calls Procedure C, then Procedure C; calls Procedure D (see Application Modules A, B, C, D ... in Fig 1), this is a repeating computing and comparing to complete executing a program.

The combination of Atkinson with McManis renders claim 19 obvious.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless-
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351 (a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6B)
4/6/04

7. Claims 9, 13-16 ~~13, 16~~, 20-26, 27-31 and 33-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Atkinson et al. (US Patent No. 6,367,012 131).

Regarding claim 1, Atkinson disclosed a method for creating a secure script, comprising: a) computing a hashed value for at least one executable command in the script; FIG. 3 is a flow diagram representing a code certification or signing method for ensuring the authenticity and integrity of a computer program, code, or an executable file received over computer network, or any other computer network. (col 6, line 19-23). Process block indicates that a cryptographic digest or "hash"
(FIG. 4) of executable file is obtained or computed. (col 6, line 39-41).

b) encrypting the hashed value for each executable command.

Process block indicates that a publisher signature (FIG. 4) is formed with cryptographic digest. (col 6, line 50-51). The public key is used (see Fig.3).

c) appending the hashed value to the script.

publisher signature are attached or appended to or incorporated to executable file. (the last line of col. 6 continue to the first line of col. 7).

d) signing the control program, comprising the public key is shown in Fig.4.

8. Referring to claims 13-15 and 20-22, wherein the control program is an ActiveX control in an application program; wherein the ActiveX control is in a HyperText Markup Language (HTML) document; wherein the HTML document is downloaded from a HyperText Transfer Protocol (HTTP) server to a HTTP client.

Atkinson disclosed (see Abstract), the executable file may be of any executable form, including an executable or portable executable .exe file format, a .cab cabinet file format, an .ocx object control format, or a Java class file.

9. Regarding claim 16, Atkinson disclosed a method for executing a script

a) verifying a public key cryptography signature associated with a control program is shown in Fig. 6.

b) computing a hashed value for each executable command in a script;

A cryptographic digest or hash is determined for the code as it is received. (col 3, line 18-19),

c) decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

d) the digest is compared to the digest included in the publisher signature. (col 3, line 19-20) c) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script;

the digest is compared to the digest included in the publisher signature. (col 3, line 19-20)

e) executing the executable commands in the, script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands. A match between the digests confirms the integrity of the code. A dialog is then rendered by the recipient computer indicating who is providing the code and the certification agency that has authenticated the identity of the publisher (col 3, line 20-24). The dialog can be rendered by browser application, for example, and can include user queries as to whether to open or run executable file. (col 8, line 24-26).

Regarding claim 23, which is a processor instructions claim as per claim 9.

Regarding claims 24, which is a processor instructions claim as per claim 16.

Regarding claims 25, which is an apparatus claim as per claim 9.

Referring claim 25, it is inherent to have a database for housing and serving the web pages.

Regarding claims 26, which is an apparatus claim as per claim 16.

Referring to claim 27, all of the steps recited in the instant claim are recited in claim 23 and are subject to the same rejection.

10. Claim 33 recites the steps of claim 16 and therefore is rejected based on the same teachings of Atkinson.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 17 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al. (US Patent 6,367,012 131, "Atkinson" hereinafter) in view of Ogilvie (US Patent 6,324,650 B1).

Regarding the instant claims, Atkinson disclosed the signed hashed value appended to the script. Atkinson, however, does not teach encrypting the script with a symmetric encryption key. Ogilvie disclosed that the system may encrypt (or reencrypt) the information during an optional encrypting step 312 to secure the sensitive information. The disclosure conditions, formats, and/or destinations may also be encrypted (col 10, line 57-59). Possible formats include plaintext, digitally signed, encrypted, XML or HTML, and other formats for electronic documents (col 10, line 19-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the script with a symmetric encryption key to secure the sensitive data as taught in Ogilvie.

Regarding claim 17, wherein the script is an encrypted script, further comprising decrypting the encrypted script with a symmetric encryption key to obtain the script. The encrypted script using a symmetric encryption key has to be decrypted with a symmetric encryption key to obtain the script.

13. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al. (US Patent 6,367,012 B1) in view of McManis (US Patent 6,546,487 131).

Regarding claim 19, Atkinson disclosed (a) computing a hashed value; (b) decrypting an encrypted hashed value appended to the script; (c) comparing the computed hashed value with decrypted hashed value. Atkinson failed to teach repeating computing (a) and comparing (c) to prevent dynamic modification. McManis disclosed a single digital signature for each program module, and the associated message digest is computed using a hash function (col 4, line 55-57). The digital signature must match corresponding message digest computed by the verifier in order the verifier to return a verification confirmation message, and then to execute the program procedure calls (col 4, line 66-67, continue to the first line of col 7, abstract). The Procedure A calls Procedure B, then Procedure B calls Procedure C, then Procedure C; calls Procedure D (see Application Modules A, B, C, D ... in Fig 1), this is a repeating computing and comparing to complete executing a program.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to repeat computing (a) and comparing (c) in order to complete executing a program/script. This repeating prevents dynamic modification to a program/script so that the integrity of a script in an application is accomplished.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the TC 2100 receptionist whose telephone number is (703) 305-3900.

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100